CENS

CENTRO NACIONAL EN SISTEMAS DE INFORMACIÓN EN SALUD

Guía Introductoria de Buenas Prácticas de Privacidad y Seguridad de Datos en Salud

Agencia Nacional de Investigación y Desarrollo
Ministerio de Ciencia, Tecnología, Conocimiento e Innovación
Gobierno de Chile

UNIVERSIDAD DE CHILE

PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE

Universidad de Concepción

Universidad de Valparaíso CHILE

TALCA UNIVERSIDAD CHILE

Versión

Versión	Fecha	Descripción	Responsable
1.0	2024	Generación de Guía	Equipo CENS

CENTRO NACIONAL EN SISTEMAS DE INFORMACIÓN EN SALUD

Indice

Glosario

- CID: Confidencialidad, Integridad y Disponibilidad.
- SGPI/PIMS: Sistema de Gestión de Privacidad de Información o Privacy Information Management System.
- SGSI/ISMS: Sistema de Gestión de Seguridad de Información o Information Security Management System.
- PHI: Información de Salud Protegida o Protected Health Information.
- IIP/PII: Información de Identificación Personal o Personally Identifiable Information.
- HIPAA Privacy Rule: Health Insurance Portability and Accountability Act/Ley de Portabilidad y Responsabilidad del Seguro Médico (Estadounidense).
    - El número (6 dígitos) se refiere a la sección del reglamento que aborda dentro de HIPAA.
    - La letra hace referencia al subtítulo dentro de esa sección.
    - El número hace referencia al inciso que especifica el contenido.
- ISO: International Organization for Standardization/Organización Internacional de Normalización.
    - El número se refiere a la sección de la ISO.

Resumen

La protección de la privacidad de datos y la seguridad de la información en el sector salud son fundamentales para garantizar la confidencialidad, integridad y disponibilidad de la información sensible. Aunque estas áreas comparten características, abordan aspectos distintos en la gestión y protección de datos personales y clínicos.

Es crucial establecer estructuras internas independientes, pero interrelacionadas para gestionar la privacidad y la seguridad de la información en salud. Un Sistema de Gestión de Privacidad de Información (SGPI/PIMS) protege los derechos individuales en el manejo de datos personales y médicos, mientras que un Sistema de Gestión de Seguridad de Información (SGSI/ISMS) protege la información crítica de la organización contra amenazas cibernéticas y otras.

Normativas como HIPAA establecen requisitos específicos para la protección de la Información Médica Protegida, integrando privacidad y seguridad. Para una protección efectiva se deben implementar recomendaciones como asignar responsabilidades claras, proporcionar capacitación adecuada, considerar ciberseguridad y establecer relaciones contractuales claras con terceros.

Enfocarse en la privacidad y seguridad en el ámbito de la salud no solo protege a las organizaciones y sus datos, sino que también asegura los principios fundamentales de la atención médica para los pacientes. Esta Guía Introductoria busca establecer recomendaciones prácticas y directrices claras para su implementación.
Las recomendaciones fueron elaboradas por el Centro Nacional en Sistemas de Información en Salud (CENS), con la colaboración de expertos y profesionales del sector, para promover las mejores prácticas y garantizar un entorno seguro y confiable para el manejo de datos sensibles en el ámbito de la salud.

En los anexos de esta guía se incorporan:

- Explicación del hacking ético, su importancia en la identificación y corrección de vulnerabilidades para mejorar la seguridad de sistemas y redes, siguiendo normas legales y éticas.
- Descripción de la normativa chilena vigente sobre la protección de datos en el sector salud, resaltando las leyes y directrices técnicas que deben seguir las instituciones para garantizar la privacidad, seguridad y calidad de la información y atención a los pacientes.
- Resumen de las regulaciones del Ministerio de Salud de Chile sobre la seguridad de la información, destacando las políticas para proteger la integridad, confidencialidad y disponibilidad de los activos de información en el sector salud.

Colaboradores:

PhD. Gastón Marquez, Académico en la Facultad de Ciencias Empresariales de la carrera de Ingeniería Civil en Informática de la Universidad del Bío-Bío. Doctorado en Informática de la Universidad Técnica Federico Santa María, Magíster en Ciencias de la Computación, Ingeniero Civil en Informática de la Universidad del Bío-Bío.

Carlos Ormeño, MSc in Advanced Computing Internet Technologies with Security, University of Bristol, Magíster en Innovación, Pontificia Universidad Católica de Chile CISM | CDPSE | LA-27.001 | C|EH.

María Erices, Coordinadora Calidad de Software en Complejo Asistencial Dr. Sótero del Río.

Equipo CENS:

PhD. Eric Rojas, Líder del Área de Calidad, Doctor en Ingeniería con mención en Computación, Académico del Departamento de Laboratorio Clínico, Facultad de Medicina e Instituto de Ingeniería Biológica y Médica de la Pontificia Universidad Católica de Chile.

Dra. May Chomalí, Directora Ejecutiva del CENS. Médica Cirujana, Especialista en Salud Pública de la Universidad de Chile y Diplomada en Gestión de Instituciones en Salud.

Priscilla Vergara, Ingeniera de Operaciones Área de Calidad, Tecnóloga en Informática Biomédica y Diplomada en Ciberseguridad.

Kenny Santibáñez, Ingeniera de Operaciones Área de Calidad y Tecnóloga en Informática Biomédica.

Privacidad de Datos y Seguridad de la Información en salud

La privacidad de datos y la seguridad de la información surgen como respuestas a riesgos específicos que pueden provocar impactos significativos, requiriendo intervenciones inmediatas y de alto nivel por parte de las organizaciones para hacer control de daños. Aunque comparten características sustanciales, es importante reconocer que la privacidad, al considerarse una propiedad de la información, se suma a la tríada de Confidencialidad, Integridad y Disponibilidad (CID) en el ámbito de la Seguridad de la Información.

La seguridad y la privacidad son dos áreas importantes para proteger la información. Aunque son diferentes, se intersectan en otorgar garantías ligadas al adecuado resguardo de los datos. La privacidad se ocupa de ámbitos específicos, como decidir qué información en un sistema de salud se puede compartir y/o quién puede acceder a ella, así como velar por la trazabilidad y derechos sobre los datos ligados a la identificación de personas. Es por ello que esta área se considera una disciplina distinta, debido a sus riesgos únicos asociados, que afectan principalmente a las personas dueñas de los datos, así como a las organizaciones encargadas de custodiarlos y/o procesarlos [1].

Por otro lado, la seguridad de la información se enfoca en prevenir el acceso a la información por parte de terceros no autorizados, velar por la integridad de la información resguardada o en tránsito, así como por la disponibilidad de la información a través de sus soportes físicos y/o tecnológicos correspondientes. Todo lo anterior, busca asegurar que las organizaciones y sus partes interesadas puedan llevar adelante su operación de forma segura y bajo un ámbito de gobernanza adecuado. Aunque estas áreas se superponen, son distintas en sus enfoques. La privacidad se relaciona con resguardar y garantizar el correcto acceso a los datos, su procesamiento y los derechos de sus dueños, mientras que la seguridad de la información busca garantizar la identificación y gestión apropiada de los riesgos a los que la información se expone, de la mano el aseguramiento de una correcta operación de la organización [2].

La vulnerabilidad de la privacidad de datos, cuando no es gestionada adecuadamente mediante tecnologías de información, puede tener consecuencias significativas. Esto va más allá de simplemente perder la confianza en productos y/o servicios, ya que puede afectar procesos, por ejemplo democráticos, como plebiscitos o elecciones, con efectos irreversibles para quienes se ven afectados.

Este impacto es especialmente crítico en el sector salud, donde la información que se maneja es altamente sensible y privada. La información se considera un activo valioso que debe protegerse correctamente. Cuando no se logra esto, una o más de las propiedades de disponibilidad, confidencialidad, integridad y/o privacidad de datos pueden verse comprometidas, afectando la calidad de la atención y seguridad de los pacientes. Esto puede traducirse en una vulneración a los derechos fundamentales de un paciente, en pérdida de oportunidades para la toma de decisiones clínicas, en resistencia en los equipos de salud debido a la desconfianza en nuevas tecnologías y en un aumento en los costos debido a servicios interrumpidos, entre otros problemas. En resumen, la gestión inadecuada de la privacidad de datos no solo afecta la confianza, sino que también tiene repercusiones significativas en la calidad de la atención médica y la seguridad de los pacientes [3].

Diferencias y convergencias entre seguridad de información y privacidad de datos.
Fuente: [1] Adaptación propia desde NIST Privacy Framework v1.0.

De esta forma, estableciendo que la privacidad y seguridad tienen un foco de medición de impacto diferente, se puede establecer que las organizaciones requieren dos estructuras internas independientes, como lo indica la Figura 1. Sin embargo, estas deben estar estrechamente relacionadas, reforzando la optimización de riesgos y recursos, así como la obtención de beneficios que generen valor para la satisfacción de las partes interesadas[4]. Para llevar a cabo lo mencionado anteriormente, es esencial que estas estructuras se instalen en la organización como Sistemas de Gestión. La noción de "Sistemas de Gestión", según la normativa ISO 9000, se define como un conjunto de elementos interrelacionados en una organización, que interactúan con el propósito de establecer políticas, objetivos y procesos para alcanzar metas específicas. En este contexto, los sistemas deben controlar la privacidad y la seguridad, abarcando aspectos de gobernanza y gestión [5]. Esto asegura una coordinación efectiva y eficiente para alcanzar los objetivos predefinidos con respecto a la privacidad y seguridad en la organización.

A continuación, la Tabla 1 destaca las diferencias en objetivos y alcance entre un Sistema de Gestión de Privacidad de Información (SGPI/PIMS) y un Sistema de Gestión de Seguridad de Información (SGSI/ISMS):

	SGPI - PIMS	SGSI - ISMS
Objetivo	Mitigar el impacto sobre las personas, que puede ser causado por un mal tratamiento de sus datos personales. Es fundamental proteger la privacidad de los datos personales, asegurando que sólo los individuos autorizados tengan acceso a esta información.	Mitigar el impacto sobre la organización, que puede ser causado por una vulneración de la confidencialidad, integridad y disponibilidad (CID) sobre su información crítica. Es esencial implementar medidas proactivas, como monitorear, revisar, mantener y mejorar la seguridad de la información de una organización, según los estándares de la norma ISO 27.000.
Alcance	Todos los procesos, tecnología y personas, independiente de su criticidad para el negocio, que tienen participación en el procesamiento o uso de Información de Identificación Personal (PII), o en el contexto de este ejercicio, de Información Médica Protegida (PHI).	La información que circula a través de los procesos críticos de la organización, esencial para gestionar el acceso a la misma, se encuentra respaldada por la tecnología. Esta tecnología no solo brinda soporte a la información, sino que también facilita la minimización de riesgos asociados a su manejo y protección.

Tabla 1. Diferencias de objetivo y alcance entre un SGPI/PIMS y un SGSI/ISMS.

Si bien en la tabla 1 se plantean diferencias entre un PIMS/SGPI y un SGS/ISMS, es fundamental reconocer que ambos deben coordinar esfuerzos para mitigar los riesgos asociados a la seguridad de los datos personales. Para facilitar la disponibilidad de un SGPI, que brinde las garantías indicadas en la gestión de datos personales, resulta crucial implementar un SGSI de manera complementaria.

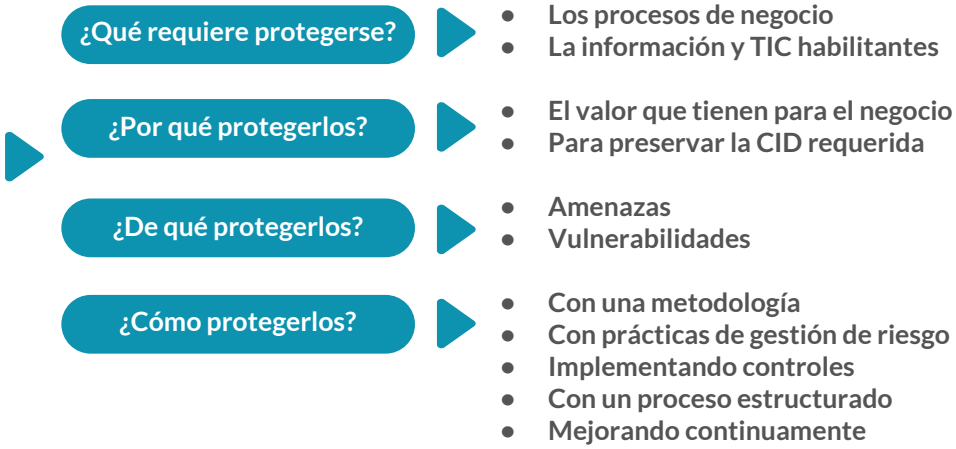
Este objetivo común encuentra su alcance en los procesos de control que velan por la confidencialidad, integridad y disponibilidad de la Información de la Identificación Personal (PII) o Información Médica Protegida (PHI) que toman parte en actividades de procesamiento o uso de ésta [6].

En este contexto, un Sistema de Gestión de Privacidad de Información (SGPI) asume la responsabilidad central de la gestión del riesgo asociado a la privacidad, particularmente en el procesamiento de la Información de Salud Protegida (Protected Health Information, PHI). Este proceso abarca el ciclo completo de vida de la información, desde la recolección de datos hasta su eliminación [7].

Tanto el SGPI como el Sistema de Gestión de Seguridad de Información (SGSI) deben coordinar sus esfuerzos para lograr sus objetivos. Mientras que el SGPI se enfoca en la privacidad, el SGSI se encarga de la seguridad de la información en general. Implementar ambos sistemas de manera complementaria es esencial para garantizar un enfoque integral en la gestión de riesgos y protección de datos.

"Es un sistema que determina: qué requiere protegerse, por qué, de qué debe ser protegido y cómo protegerlo."

Albert, 2003



Fuente: Managing Security Risk - Cristopher Albert 2003

Uso y Procesamiento de PHI (Información de Salud Protegida)

La Información de Salud Protegida se refiere a datos que permiten identificar de manera individual a una persona. Esto incluye información demográfica y detalles sobre su estado de salud física o mental, tanto en el pasado como en el presente o futuro, así como información relacionada con servicios de atención médica. En términos más sencillos, se trata de información que individualiza a una persona y abarca aspectos de su salud y atención médica.

Para establecer de forma precisa el alcance de la gestión de la privacidad, centralizada en un Sistema de Gestión de Privacidad de Información (PIMS), se debe identificar y justificar el grado de responsabilidad dentro del ciclo de actividades de uso y procesamiento de la Información de Salud Protegida (PHI), en función de las actividades específicas que ejecuta en este contexto. En este punto, los diferentes marcos normativos y regulatorios para privacidad, coinciden en que existen tres roles principales en un esquema de uso o tratamiento de datos, dentro de los cuales se encuentran: "Entidades Cubiertas o Covered Entities", los "Socios Comerciales o Business Associate", y los "Individuos o Individuals". Aunque las definiciones detalladas de estos conceptos se encuentran en la sección de glosario de la HIPAA Privacy Rule, es esencial destacar las diferencias, especialmente en lo que respecta a las responsabilidades en el uso de la PHI. A continuación, se describen estas diferencias para una comprensión más clara.

Entidad Cubierta: Corresponde a la entidad proveedora de servicios de salud que ejecuta las actividades de recolección, obtención del consentimiento y definición del propósito de la PHI, y por ende, actúa como responsable de proteger la privacidad y seguridad de la información, junto con la mitigación del impacto que pueda derivarse del procesamiento o uso de esta desde su recolección hasta su eliminación.

Socios Comerciales: Corresponde a una entidad que realiza ciertas funciones o actividades, que involucran el uso de PHI en nombre de una Entidad Cubierta, o que presta servicios a ella. Los Socios Comerciales no recolectan los datos directamente, sino que los obtienen a través de una relación contractual con la Entidad Cubierta, mediante la cual se define el alcance y atributos de tratamiento o uso que tienen estas sobre la PHI, siendo directamente responsables del cumplimiento de la normativa

Individuo: Persona a la que hace objeto la PHI, o dicho de otra forma, persona que hace entrega de sus datos personales bajo una declaración de consentimiento explícita entregada a la Entidad Cubierta.

En función a lo anterior, la institución debe poseer facultades para ejecutar actividades relacionadas al uso o procesamiento de PHI, las cuales se deben encontrar delimitadas contractualmente, en base al propósito de tratamiento definido por las Entidades Cubiertas, y que excluyen aquellas actividades relacionadas con la recolección de datos directamente desde los individuos, y por ende la obtención de su consentimiento.

Recomendaciones para Gobierno y Gestión de la Privacidad

Para establecer un análisis que facilite su entendimiento e interpretación, se definieron los siguientes Principios de Privacidad Generales, los que representan los pilares sobre los cuales se debe construir un marco de privacidad gestionado y gobernado, que vele por la prevención y la mitigación del impacto hacia las personas o individuos, del procesamiento o uso de la PHI, utilizando como pivote la conexión normativa dada por la ISO/IEC 27.701 [8] y por HIPAA Privacy rule, 2022 [6].

1. Principio de Privacidad por Diseño
Este principio establece las directrices para la incorporación de la privacidad de información como parte basal en la organización a través de un PIMS, considerando una conexión sólida con la Seguridad por Diseño plasmada a través de un SGSI.

Directrices / Lineamientos	Recomendaciones de Implementación	ISO 27.701 (Sección)	HIPAA PR [Sección-(subtítulo (inciso))]
Asignación de responsabilidades	Se debe establecer una estructura funcional dedicada a la gestión y gobierno de la privacidad de información, centralizada en un PIMS, la cual defina roles y responsabilidades para la gestión del programa de privacidad al interior de la empresa o institución, tomando en cuenta los aspectos conjuntos a trabajar con el SGSI.	8.5	164.530(a)(1)
Entrenamiento y awareness	Se deben establecer procesos de entrenamiento y concientización en materias de privacidad, de forma que los roles internos que participan en las actividades de procesamiento o uso de la PHI eleven su nivel de madurez en este aspecto.	6.4.2.2	164.504 164.530
Consideraciones de ciberseguridad	Incorporar un proceso de gestión de riesgos de privacidad, que permita establecer los requisitos de aseguramiento de la tecnología involucrada en el procesamiento de PHI.	8.4	164.504 164.530

2. Principio de Individuos

Este principio establece las directrices para involucrar directamente a los individuos en el procesamiento y uso responsable y legal de su PHI

Directrices / Lineamientos	Recomendaciones de Implementación	ISO 27.701 (Sección)	HIPAA PR [Sección-(subtítulo (inciso))]
Consentimiento en el procesamiento y uso de PHI.	Se debe establecer procesos que garanticen: • Que los aspectos de tratamiento que se realicen estén declarados en el objetivo que la Entidad Cubierta transparente a los Individuos. • Que el procesamiento que se le da a la PHI aborde solo lo declarado en el consentimiento establecido entre la Entidad Cubierta y los Individuos.	8.5.7	164.506(c) (1-4)
Posibilidad de objeción.	Se debe comunicar a las instituciones ante cualquier cambio en el procesamiento de PHI que se escape de lo definido en la declaración de objetivo de procesamiento mediante la cual los Individuos entregan su consentimiento, de forma que las Entidades Cubiertas puedan comunicar estos cambios en el objetivo a los Individuos, para que estos puedan dar su aceptación u objeción.	8.5.7	164.508 164.510 (a)(2) 164.510 (b)
Relación contractual.	Se deben especificar detalladamente las actividades de procesamiento y uso que realizará la institución sobre la PHI de los individuos, de modo que el individuo tenga la oportunidad de aceptar, prohibir y/o restringir su uso. Es crucial considerar con detalle las actividades de procesamiento y uso que la institución llevará a cabo con la PHI de los individuos.	8.5.7	164.506(c) (1-4) 164.510 (a)(2) 164.510 (b)

3. Principio de Minimización de entrega de Datos

Este principio establece las directrices para limitar, al mínimo posible, la entrega de datos entre las entidades que procesan PHI de los Individuos, en función del objetivo de procesamiento declarado.

Directrices / Lineamientos	Recomendaciones de Implementación	ISO 27.701 (Sección)	HIPAA PR [Sección-(subtítulo (inciso))]
Entrega limitada de PHI.	Se debe establecer un mapeo o relación entre la PHI requerida y las actividades de procesamiento que se le da, de forma de limitar la PHI que las Entidades Cubiertas entregan al mínimo.	8.2.1	164.506
Identificación de la regulación.	Se debe identificar y documentar la regulación a la cual se encuentra la empresa o institución en el contexto del procesamiento o uso de PHI, de forma de transparentar a los Individuos el marco legal en el que se sustentan las prácticas de privacidad.	8.1 8.2 8.2.1 8.5.1 8.5.7	164.520(a)
Restricción interna para el procesamiento de PHI.	Se debe identificar qué áreas internas ejecutan actividades de procesamiento de la PHI entregada, de forma de establecer limitaciones sobre éstas en el uso y procesamiento de datos	8.2.3	164.502 164.504 164.510 164.512 164.514 164.532

4. Principio de Transparencia

Este principio establece los lineamientos para generar un ecosistema de procesamiento y uso de PHI transparente que involucre al Individuo, Entidad Cubierta y Socios Comerciales.

Directrices / Lineamientos	Recomendaciones de Implementación	ISO 27.701 [Sección]	HIPAA PR [Sección]
Uso de medios digitales.	Se deben utilizar los medios digitales, como página web, aplicaciones móviles, entre otros, para comunicar al público general la información relacionada con las actividades de uso o tratamiento sobre PHI.	8.2.2 8.5.1	164.520
Especificación del propósito.	Se deben transparentar de forma detallada, el o los propósitos para los cuales se ejecuta el procesamiento y uso de PHI, explicando al individuo como se usará o divulgará la información de salud protegida	8.2.2 8.5.1	164.520

5. Principio de procesamiento seguro de datos
Este principio entrega las directrices para establecer un procesamiento seguro de la PHI, desde el momento en que es transferida, hasta que esta finaliza su ciclo de vida dentro de la organización.

Directrices / Lineamientos	Recomendaciones de Implementación	ISO 27.701 (Sección)	HIPAA PR [Sección-(subtítulo (inciso))]
Procesamiento seguro de PHI.	La PHI al interior de la organización, se debe trabajar de forma protegida, utilizando mecanismos de anonimización, pseudo anonimización y minimización de datos, que permita proteger la información contra el acceso no autorizado, corrupción o pérdida durante todo su ciclo de vida . Implica el uso de herramientas y tecnologías.	N/A	164.514(a) 164.514(b)

6. Principio de Derechos del Individuo
Este principio establece las directrices para garantizar un acceso adecuado y oportuno de los Individuos a su PHI.

Directrices / Lineamientos	Recomendaciones de Implementación	ISO 27.701 (Sección)	HIPAA PR [Sección-(subtítulo (inciso))]
Actualización de PHI	Se deben establecer procesos eficientes que permitan una actualización de la PHI en función de los requerimientos del individuo. En este punto, se debe establecer este proceso basado en la comunicación con la Entidad Cubierta, siendo ésta, la responsable de recibir y canalizar los requerimientos de los Individuos.	8.2.5	164.526
Notificación de actualizaciones sobre PHI	Se debe establecer un proceso de notificación para todas las partes interesadas que estén vinculadas a la PHI que se actualizó, en función de los requerimientos del Individuo. Esta comunicación debe ir orientada a la Entidad Cubierta para que ésta notifique al Individuo, así como a cualquier tercera parte interesada o requerida.	8.5.8	164.526

7. Principio de Gestión de Terceras Partes

Este principio establece los lineamientos para el involucramiento controlado de terceras partes que puedan tener acceso a la PHI, y con más énfasis aún, si estos ejecutan actividades de procesamiento o uso sobre ésta.

Directrices / Lineamientos	Recomendaciones de Implementación	ISO 27.701 [Sección]	HIPAA PR [Sección]
Gestión de terceros	Se deben establecer mecanismos de transmisión segura de la PHI cuando ésta va a ser procesada por un tercero velando por mantener el principio de recolección mínima de datos mencionado anteriormente.	8.4.3 8.5.1 8.5.7	164.502 164.504
Relación contractual	Se deben establecer términos y condiciones contractuales que apoyen de forma de establecer el objeto del tratamiento. Las relaciones contractuales con terceros deben ser notificadas de forma detallada a las Entidades Cubiertas, considerando su objeto, minimización de datos y alcance de uso y procesamiento.	8.2.5 8.5.8	164.502 164.504 164.514

Conclusión

El sector de la salud ha experimentado un progreso significativo en la implementación de diversas tecnologías y sistemas de información, por lo que es crucial adoptar mecanismos que gestionen y resguarden la información personal y clínica. La privacidad de datos y la seguridad de la información en salud son conceptos interrelacionados, pero con enfoques y aplicaciones distintas. La necesidad de gestionar y proteger la información en entornos de salud es imperativa debido a riesgos específicos. Aunque comparten aspectos como la confidencialidad, integridad y disponibilidad, la privacidad agrega una dimensión ética y legal más profunda.

En este contexto, si bien la privacidad de datos y la seguridad de la información se relacionan, lo cierto es que tienen enfoques distintos. Mientras que la seguridad de la información protege sistemas y datos de amenazas maliciosas, la privacidad se centra en asegurar los derechos individuales en la recopilación, uso y divulgación de datos personales y clínicos. A pesar de sus diferencias, su conexión es esencial para garantizar la privacidad, seguridad y el adecuado tratamiento de los datos en el sector de la salud.

Para gestionar la privacidad y seguridad de la información en salud, es esencial establecer estructuras internas independientes, pero vinculadas. Un Sistema de Gestión de Privacidad de Información (SGPI/PIMS) se enfoca en mitigar el impacto en las personas, debido al manejo de sus datos personales y médicos. Por otro lado, un Sistema de Gestión de Seguridad de Información (SGSI/ISMS) se dedica a proteger la confidencialidad, integridad y disponibilidad de la información crítica de la organización. Normativas como HIPAA buscan prevenir accesos no autorizados a la Información Médica Protegida, integrando estratégicamente la privacidad y la seguridad.

Esta protección se logra mediante la aplicación de principios clave como la privacidad por diseño, involucramiento de individuos, minimización de datos, transparencia y procesamiento seguro de datos, entre otros. Estos principios se implementan con recomendaciones específicas, incluyendo asignación de responsabilidades, capacitación, consideraciones de ciberseguridad y más. En última instancia, enfocarse en la privacidad y seguridad en el ámbito de la salud no solo resguarda a las organizaciones y sus datos, sino que también asegura los principios fundamentales de la atención de salud para los pacientes. Esto implica respetar los derechos individuales, generar confianza en los sistemas de atención médica, proteger datos y garantizar el acceso a una atención oportuna y de calidad, contribuyendo directamente a preservar la calidad de vida personal y social.

Bibliografía

[1] NIST, v1.0 (2020). Diferencias y convergencias entre seguridad de información y privacidad de datos. Obtenido de *https://www.nist.gov/privacy-framework*

[2] NISTIR 8062 (2017). An Introduction to Privacy Engineering and Risk Management in Federal Systems. Obtenido de *https://csrc.nist.gov/publications/detail/nistir/8062/final*

[3] European Parliament and Council of the European Union. (2016). General Data Protection Regulation (GDPR). Obtenido de *https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679.*

[4] ISACA. (2018). COBIT 2019 Framework: Governance and Management Objectives. Obtenido de *https://www.isaca.org/bookstore/bookstore-cobit-digital/whpcb19.*

[5] International Organization for Standardization. (2015). ISO 9000:2015 Quality management systems - Fundamentals and vocabulary. Obtenido de *https://www.iso.org/standard/45481.html.*

[6] U.S. Department of Health and Human Services. (2003). HIPAA Privacy Rule, 45 CFR Parts 160 and 164. Obtenido de *https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.*

[7] National Institute of Standards and Technology. (2020). NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0 Obtenido de *https://www.nist.gov/privacy-framework.*

[8] International Organization for Standardization. (2019). ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. Obtenido de *https://www.iso.org/standard/71670.html.*

[9] Ministerio de Salud de Chile. (2021). Resolución Exenta N° 785: Aprueba Instructivo de Seguridad de la Información y Ciberseguridad para el Sector Salud. Obtenido de *https://www.minsal.cl/wp-content/uploads/2015/08/Res.Ex_.-N%C2%B0-785-03.11.2021-Aprueba-Instructivo-de-Ciber-para-Sector-Salud.pdf.*

[10] National Institute of Standards and Technology. (2020). NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. Obtenido de *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.*

[11] Ministerio de Salud de Chile. (2015). Política General de Seguridad de la Información. Obtenido de *https://www.minsal.cl/seguridad_de_la_informacion/.*

[12] Ministerio de Salud de Chile. (2015). Política de Protección de Datos Personales. Obtenido de *https://www.minsal.cl/seguridad_de_la_informacion/.*

[13] Ministerio de Salud de Chile. (2015). Política de Desarrollo de Sistemas Seguros. Obtenido de *https://www.minsal.cl/seguridad_de_la_informacion/.*

Anexos

1. Hacking Ético

Se considera hacking ético como una práctica autorizada para detectar vulnerabilidades, debilidades y/o errores de diseño o flujo en una aplicación, sistema o infraestructura de una organización, con la finalidad de eludir la seguridad del sistema para identificar oportunidades de mejora de cara a los flujos, datos, diseño e implementación del objetivo analizado. En general, los hackers éticos tienen como objetivo investigar y analizar el sistema o la red en busca de puntos débiles que los ciberdelincuentes puedan explotar. A su vez, desde una óptica organizacional, ayudan a las organizaciones a elevar su nivel de madurez por medio de la mejora de los procesos operacionales, de seguridad y/o ciberseguridad atingentes a sus alcances de evaluación y hallazgos. Algunas de las principales actividades realizadas en actividades ligadas al hacking ético son las siguientes:

- **Ataques de inyección:** Son amenazas informáticas en las que los atacantes introducen código malicioso en entradas de datos para manipular sistemas. Un ejemplo común es el ataque de inyección SQL, donde se utilizan instrucciones maliciosas para acceder o cambiar datos sin autorización.
- **Cambios en la configuración de seguridad:** Son cambios realizados en un sistema para fortalecer o debilitar sus medidas de protección, como contraseñas o políticas de acceso.
- **Exposición de datos sensibles:** Implica identificar y demostrar, de manera controlada, posibles riesgos de divulgación de información confidencial para fortalecer las medidas de seguridad de una organización.
- **Violación de los protocolos de autenticación:** Involucra detectar y mostrar de manera controlada fallos en los mecanismos de verificación de identidad, con el propósito de mejorar la seguridad, corrigiendo vulnerabilidades que podrían ser aprovechadas por actores malintencionados.
- **Componentes utilizados en el sistema o la red que puedan utilizarse como puntos de acceso:** Se refiere a componentes del sistema o red que, de manera controlada, son identificados y evaluados para detectar posibles vulnerabilidades y fortalecer la seguridad, evitando su explotación por parte de actores malintencionados.

Los hackers éticos deben seguir unas normas básicas de conducta, las cuales son las siguientes:

- Mantener la legalidad de sus actividades, obteniendo las aprobaciones adecuadas antes de acceder a los sistemas o realizar una evaluación de seguridad.
- Determinar el alcance de la evaluación para garantizar que su trabajo se mantenga dentro de límites bien definidos y aprobados por la organización.
- Informar a la organización evaluada de todas las vulnerabilidades descubiertas durante su evaluación, así como proporcionar información completa, que permita y facilite una adecuada gestión de remediación de los hallazgos presentados.
- Velar por la confidencialidad, integridad, disponibilidad y privacidad de la información, procesos y flujos operacionales a los que tiene acceso. Lo anterior, se debe garantizar mediante instrumentos legales, como un Acuerdo de No Divulgación (NDA por sus siglas en inglés), así como condiciones contractuales acordadas y aceptadas de forma previa al inicio de los ejercicios.

En resumen, el hacking ético implica la búsqueda autorizada de vulnerabilidades, debilidades y/o errores en sistemas y aplicaciones con el objetivo de mejorar su seguridad, siendo una buena práctica para fortalecer las defensas y prevenir posibles ataques. Los hackers éticos analizan y estudian sistemas en busca de vulnerabilidades, llevando a cabo actividades como ataques de inyección, ajustes en la configuración de seguridad, identificación controlada de exposición de datos sensibles y detección de fallas en protocolos de autenticación. Es esencial que sigan pautas éticas, obtengan aprobaciones legales, establezcan límites claros en sus evaluaciones, informen sobre vulnerabilidades y respeten la confidencialidad de los datos, contribuyendo así a la seguridad integral de los sistemas y al aseguramiento de la continuidad operacional de los objetivos evaluados.

2. Regulación chilena sobre los Datos

La normativa actual del MINSAL describe que los sistemas de información de salud que se implementan para instituciones de salud deben garantizar la privacidad del paciente y dar estricto cumplimiento a los estándares técnicos que el MINSAL determine respecto a metodologías que permitan cumplir con estándares de seguridad de la información y calidad de atención de los pacientes en base a las leyes N 19.628 y 20.584.

Por otro lado, por decreto del Ministerio Secretaría General de la Presidencia, establece como norma técnica sobre la seguridad de la información de los documentos electrónicos, fijar las directrices generales que orienten la materia de seguridad dentro de cada institución que refleje claramente el compromiso, apoyo e intereses en el fomento y desarrollo de una cultura de seguridad institucional, lo que aplica los a los sistemas de información de salud.

A su vez, por resolución exenta N 785, se aprobó un instructivo de seguridad de la información y ciberseguridad [9] *(www.minsal.cl/wp-content/uploads/2015/08/Res.Ex_.-N%C2%B0-785-03.11.2021-Aprueba-Instructivo-de-Ciber-para-Sector-Salud.pdf)* para el sector salud cuyo objetivo es entregar lineamientos para la implementación de una base de seguridad de la información y ciberseguridad en las Secretarías Regionales Ministeriales de Salud, Servicios de Salud y Establecimientos relacionados que permitan resguardar la confidencialidad, integridad y disponibilidad de la información de las actividades realizadas para la gestión de servicios, teniendo en cuenta la norma chilena “NCH-ISO 27001. Of. 2013”, marco de seguridad del NIST “Controles SP 800-53” y líneas base de control “SP 800-53B” [10].

Finalmente, el gobierno menciona que la gestión de la seguridad de la información es un imperativo que se debe cumplir en el marco de la normativa gubernamental vigente, el cual requiere actualizar las políticas de seguridad de acuerdo a las metodologías y estándares técnicos que permitan lograr niveles de integridad, confidencialidad y disponibilidad con todos sus activos relevantes para las instituciones.

3. Reglamentos del Ministerio de Salud (Minsal) respecto a la Seguridad de la Información

En la actualidad, la diversidad de activos de información institucional, que comprende desde documentos en papel hasta sistemas digitales, bases de datos, equipos informáticos y redes de transmisión de datos, se encuentra expuesta a varios riesgos tanto internos como externos a la organización. Estos riesgos subrayan la necesidad de implementar medidas de seguridad efectivas para preservar la integridad, confidencialidad y disponibilidad de la información.

En agosto de 2015, el Ministerio de Salud (Minsal) establece regulaciones clave que abordan tres áreas fundamentales:

- **Política general de seguridad de la información:** Tiene como propósito establecer directrices para proteger integralmente la información y los sistemas del Ministerio de Salud. Busca garantizar la confidencialidad, integridad y disponibilidad de los activos de información, al tiempo que mitiga los riesgos asociados con la ciberseguridad. [11]
- **Política de protección de datos personales:** Esta política tiene como objetivo establecer directrices para proteger la privacidad de la información personal recopilada, almacenada, procesada y transmitida en el Ministerio de Salud. [12]
- **Política de desarrollo de sistemas seguros:** Establece directrices para garantizar la seguridad en los productos de software en instituciones del sector salud. Define requisitos para desarrollos internos y externos, considerándolos en cada etapa de desarrollo y controlando los entornos de trabajo en desarrollo, pruebas y producción. [13]

Estas políticas buscan proporcionar pautas para asegurar la seguridad y privacidad de la información en el ámbito de la salud. Además, el Minsal promueve activamente la implementación de un Sistema de Seguridad de la Información con el objetivo de reducir significativamente el impacto de los riesgos en los activos de información. El propósito primordial de este sistema es garantizar niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información institucional relevante, asegurando así la continuidad operacional de los procesos y servicios mediante una gestión eficaz de la seguridad de la información.

Agencia Nacional de Investigación y Desarrollo
Ministerio de Ciencia, Tecnología, Conocimiento e Innovación
Gobierno de Chile

UNIVERSIDAD DE CHILE

PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE

Universidad de Concepción

Universidad de Valparaíso CHILE

TALCA UNIVERSIDAD CHILE